Integrating Luna/SafeNet 1700 Hardware Security Module (Luna Client 6.1 & firmware 6.2.1) w/ CyberArk Enterprise Password Vault (EPV) v9.5

The following document was developed to assist in the installation of a Luna/SafeNet 1700 PCI Express Hardware Security Module. These security roles are Security Officer (blue), domain or cloning key (red) and the partition owner (black key). This product uses small USB keys or tokens to represent its security roles. Also included is a physical PED (pin entry device). The PED hooks directly into the back of the the HSM PCI card with a proprietary serial connection. This allows you to set additional PIN codes for each of these roles if desired.

This guide will help you create a security domain on the primary HSM and then use the SafeNet backup device to backup the security domain and clone it onto the secondary HSM card. By doing so, you will ensure your primary EPV can failover to a backup site seamlessly. It also assumes that you have a dedicated, local PCI Luna HSM card installed locally in each server. As mentioned above, the 1700 model was tested which uses a 1024 RSA key and can process 1,700 digital signatures per second.

The following was tested with the Cyber-Ark Advanced Appliance on December 23, 2015.

This document was produced by CyberArk Software and assumes the following:

- A proficient level of experience with CyberArk Security Suite
- CyberArk EPV is installed on a primary and backup (DR) EPV that was previously hardened
- CyberArk PA Client Installed on both servers
- Console access to Vault server is not always available, this may also be done through RDP

  When opening a command prompt or installing any software referenced in this guide please **run as administrator.**

Section 1

Step 1:

1. Install Luna PCI Client Software

Install the HSM device into your server's PCI slot. Run the provided 64-bit software called LunaClient.msi. Make sure to include the following components.

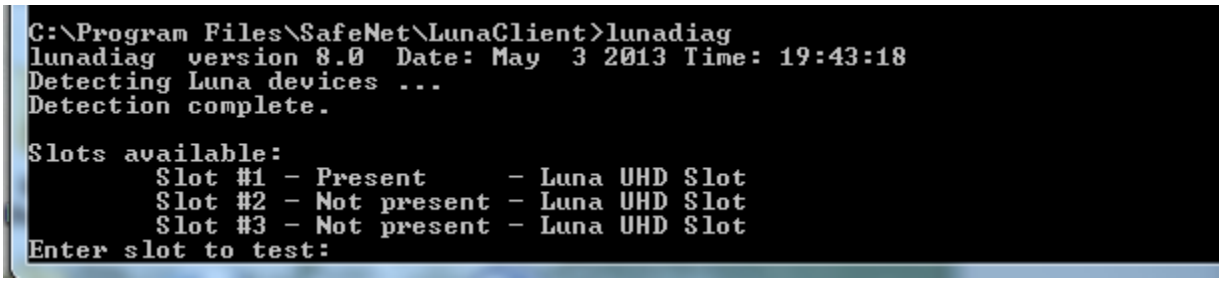
- LunaPCI
- Remote PED (not required)
- Remote Backup

2. Confirm the slot is present

Note: Type SET to ensure the variable for the installation path is present – no problem with this in the lab

From a command prompt navigate to ***C:\Program Files\Safenet\LunaClient***

type **lunadiag**

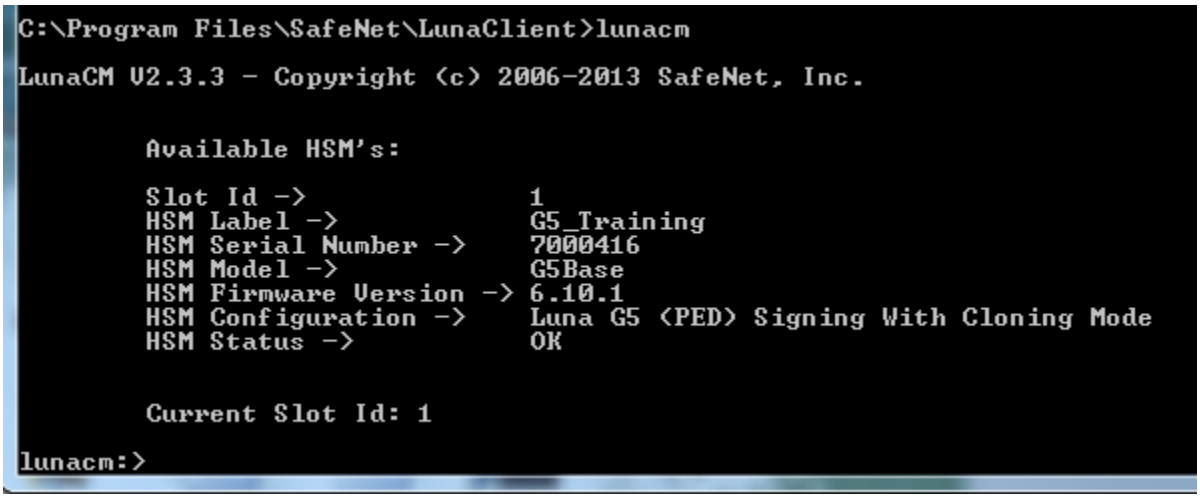


If the slot is listed as present, no further testing is necessary.

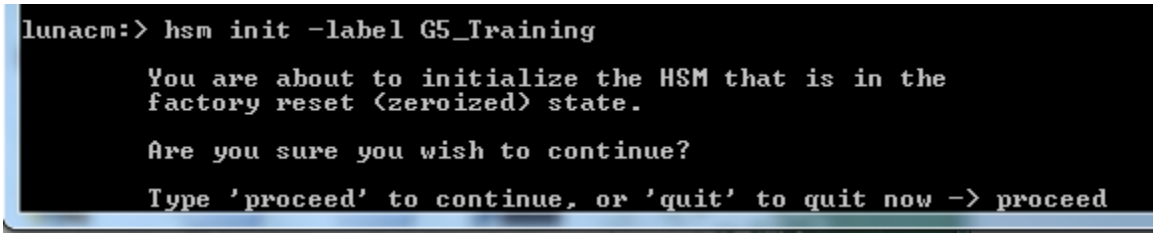
3. Initialize the LunaPCI

From *C:\Program Files\Safenet\LunaClient*
(Note: If using MofN for the PED key roles, you must first increase the PED timeout 2 in the chrystoki.ini file. Change from the default of 100000 to 700000.)

Type **lunacm**



Type **hsm init -label *<yourlabelhere>***



Type **proceed,** when prompted.

The next steps happen as a result of the HSM INIT command entered above. These activities happen on the PED as one operation.

a. Create Security Officer Key (Blue)

You will be prompted on the PED - "Would you like to use an existing keyset?"
Select ***NO***

Configure the desired M of N value *(this step will cover 1 of 1, but testing was done with MofN 2/3 for Proof of Concept)* To setup MofN such as 2/3 just enter the desired value into the PED and follow the instructions. The product ships with 10 USB security tokens and is quite flexible as to how can be setup to meet your security needs.

On the PED, select **1** (for M)
Hit *Enter*
On the PED, select **1** (for N)
Hit *Enter*

PED will prompt to insert a SO key (Blue Key)
Insert a new USB Key to be configured as (SO) security officer (Blue Key)

PED will warn you that the key is blank
Select ***YES*** to overwrite

PED will prompt for a PIN
Enter desired PIN
Confirm PIN

PED will prompt SO (Security Officer) to login – testing the PED token and PIN.
Enter your PIN

b. Create Domain Key (Red)

You will be prompted on the PED - "Would you like to use an existing keyset?"
Select ***NO***

Configure the desired M of N value *(this doc will cover 1 of 1)*
On the PED, select **1** (for M)
Hit *Enter*
On the PED, select **1** (for N)
Hit *Enter*

PED will prompt to insert Domain key (Red Key)
PED will warn you that the key is blank
Select ***YES*** to overwrite

PED will prompt for a PIN
Enter desired PIN
Confirm PIN

You will be prompted "Would you like to use an existing keyset"?
Select ***NO***
At this point, Initialization is complete

From *C:\Program Files\Safenet\LunaClient*

Type **lunacm**
Type **hsm si**

Review the information hsm information that is displayed

4. Optional – Change FIPS mode.

The device is not shipped in FIPS mode by default. Our testing was done in FIPS mode. To change the HSM into FIPS mode, carry through with this step.

From *C:\Program Files\Safenet\LunaClient*

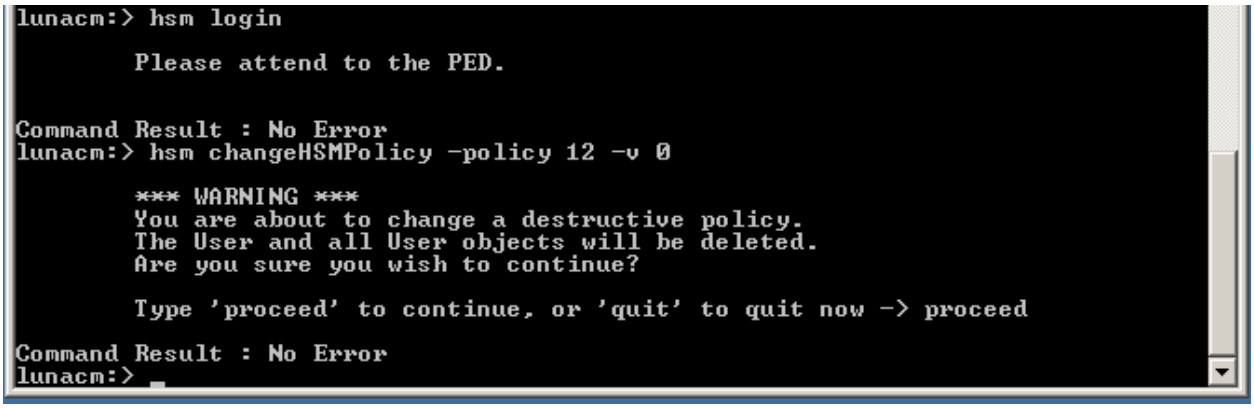
Type **lunacm**
Type **hsm showPolicies** (to get FIPS mode policy number)

Note: The policy is *12 - Enable Non-FIPS algorithm*

Type **hsm login** (to login as SO)

Enter your PIN via the PED

Type **hsm changeHSMPolicy -policy 12 -v 0**



The hsm is now in FIPS mode, type **par si** – this will confirm the device is in FIPS mode and that the partition was created successfully. User Flags -> CONTAINER_CREATED

*** The HSM is in FIPS 140-2 approved operation mode. ***

5. Create Partition on Luna PCI (black keys)

From *C:\Program Files\Safenet\LunaClient*

Type **lunacm**
Type **par crp**

See the PED for the following instructions.

a. Create Partition Owner or Crypto Officer key (Black)

PED will prompt you for a user key
You will be prompted "Would you like to use an existing keyset?"
Select ***NO***

PED will warn you that the key is blank
Select ***YES*** to overwrite

Configure the desired M of N value (this doc will cover 1 of 1)
On the PED, select **1** (for M)
Hit Enter
On the PED, select **1** (for N)
Hit **Enter**

PED will prompt for a PIN
Enter desired PIN
Confirm PIN

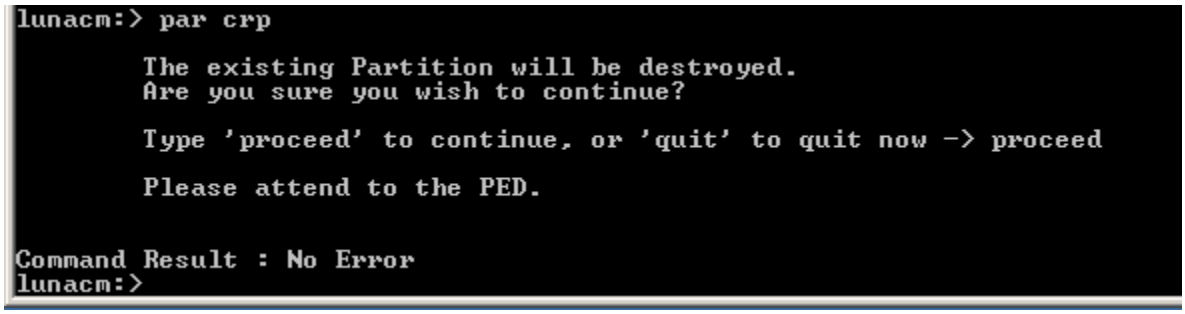
PED will prompt user (partition owner) to login
Enter your PIN
lunacm will confirm the login is successful

b. At this point you will be prompted to create or reuse a Domain Key (RED)

You will be prompted "Would you like to use an existing keyset?"
Select ***Yes*** *(to use existing HSM Domain (Red) key)*
** optional select NO, then create a second Domain key unique to the partition*

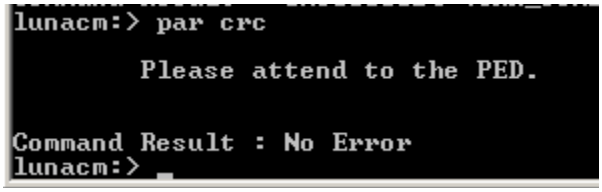
Insert the domain key
Enter the PIN

Partition will be created



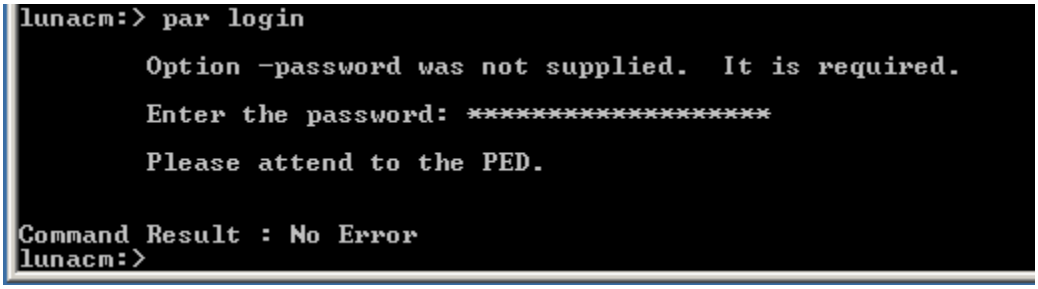
6. Create User Challenge and change it if you wish

Type **par crc**



Check the PED for the generated challenge phrase (ex. THe5-kkHT-HHRW-pqWS)
Write it down – you can disregard the "-" when entering this phrase into the prompt
Hit ***Enter*** on the PED

Type **par login**
Enter your PED generated challenge phrase
Enter your Owner key (black) in the PED and enter your PIN



You should now be logged in successfully

Change your challenge phrase to something more usable (Optional)

Note: Remember to match the PIN to the challenge phrase from both the primary and the secondary EPV

Type **par changePw -p**
Enter your old challenge phrase when prompted
Enter your new password when prompted
Confirm new password when prompted

```
lunacm:> par changePw -p

        Option -oldpw was not supplied.  It is required.

        Enter the old challenge: ********************

        Option -newpw was not supplied.  It is required.

        Enter the new challenge: *******

        Re-enter the new password: *******

        Please attend to the PED.

Command Result : No Error
lunacm:>
```

(Optional) - Change partition policies to allow activation/auto activation

This is a security feature to ensure if the server is rebooted it comes back on-line.

a. Display Partition Policies

Type **par showpolicies** (to determine the activation policy (22))

b. Change the partition policy to allow partition activation

Type **par changepolicy -p 22 -v 1**

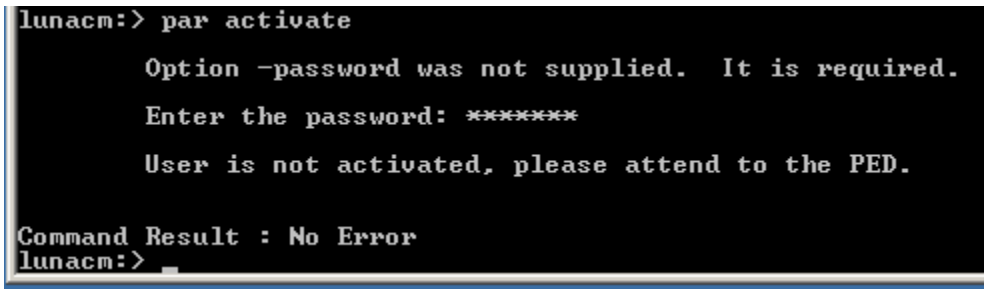
```
lunacm:> par changePolicy -policy 22 -v 1

Command Result : No Error
lunacm:>
```

c. the policy to allow auto-partition activation

Type **par changepolicy -p 23 -v 1**

d. Activate the partition

Type **par activate**
Enter Partition Owner password
Attend to the PED, insert Partition Owner USB token w/PIN (if applicable)



The partition is now activated

Step 2:

1. Reference PKCS#11 path in dbparm.ini

PKCS#11providerpath exact syntax is below:

PKCS11ProviderPath="C:\Program Files\SafeNet\LunaClient\cryptoki.dll"

2. Set a PIN through Cyber-Ark command line

Run the CAVaultManager SecureSecretFiles command to secure the code that will be used to access the Server key – **ensure this is the same password as you set in step 6 above.**

CAVaultManager SecureSecretFiles /SecretType HSM /Secret <hsmpincode>

3. Run this to confirm the key has been set propertly

CAVaultManager SecureSecretFiles /SecretType HSM /Secret (CryptoOfficer Key) CryptoOfficer Key is the language that SafeNet uses, but for CyberArk calls it an HSM pin code.
(may not need this step)

4. Open DBParm to ensure that the PIN code was added to the file successfully.

5. Stop and then start the Vault Server from the GUI.

6. Stop the Vault Server from the GUI.

7. Generate keys on the HSM device

Run the following command through elevated command line:
CAVaultManager GenerateKeyonHSM /ServerKey

Running the GenerateKeyonHSM.exe command will tell the vault to connect to the HSM and issue a "generate new key" command. Additionally, we will have to ensure that the CyberArk software configuration file (dbparm.ini) points the HSM to the proper PKCS11 libraries which we did in step 1 above. The Luna/SafeNet software package ships with 64-bit library which is compatible with this server.

Typical error if you have an incorrect library file or parameter in dbparm.ini is below:

C:\Program Files (x86)\PrivateArk\Server>CAVaultManager GenerateKeyonHSM /Server
Key
ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 b
it, RSA (2048 bit), SHA1.
ITADM114I Successfully connected to Database, Database id 0.
CAVLT137E Cannot initialize HSM provider (Code 1100, -1)
You'll see the above error if you are not using the correct PKCS11 .dll library.

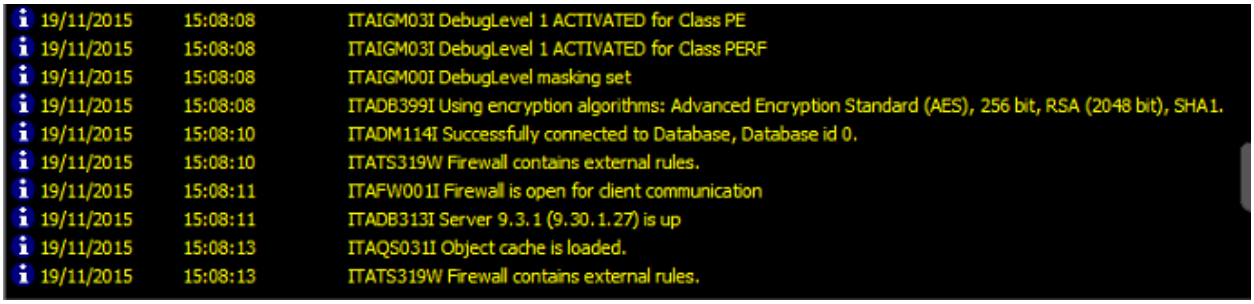
8. Run **ChangeServerKeys** command

-enter master location
-enter HSM#1 (generated from step above)
-input master directory again
-you'll have to edit the dbparm.ini as necessary to point to the recprv.key from the CD. It will error out without this step.
-Successful output will end with this note.

12/12/2015 10:42:29 CHSRVK054I ChangeServerKeys process was successful.

9. Update dbparm.ini with Serverkey=HSM#1

If service starts successfully, it will output the following and you should confirm you can log-in to the EPV as the Administrator.



Section 2: **Backing up HSM server keys onto backup device from Primary HSM**

Items required:

- PED
- Backup device connected to HSM device
- Blue, Red and Black keys

Partition Backup

	If it is not already, Activate the slot that you will be backing up. May require the PED and the Crypto Officer (BLACK) key and password	
	Connect HSM BU device to your local PC via USB cable. Connect PED to HSM BU device.	
	C:\Program Files\Safenet\LunaClient> lunacm lunacm:> slot list	List all available slots including the backup device
	lunacm:> slot set -s <slot# of Backup Device> lunacm:> hsm init -label <*label of Backup Device*> -*initWithPED*	Init the HSM backup device. **Important** make sure slot is set to backup device!! Follow PED commands HSM SO and domain key required.
	lunacm:> partition archive list -slot <slot# of Backup Device>	List the partitions on the Backup Device (if any)
	lunacm:> slot set -slot <slot# of partition to be backed up>	Point the active slot to the partition (slot) you want to backup
	lunacm:> par login	Login into the partition to be backed up as Crypto Officer
	lunacm:> partition archive backup -slot <slot# of Backup Device> partition <name of partition to be created on backup device>	Backup up the active slot Attend the PED. This process will: - Login to the Backup device with HSM SO (BLUE) key - Creates a partition on the BU device (BLACK) - Logs in to partition (BLACK) - Creates a Domain (RED) - Backs up and verifies partition contents
	lunacm:> partition archive list -slot <slot# of Backup Device>	List the partitions on the Backup Device
	lunacm:> partition archive contents -slot <slot# of Backup Device> -partition <name of partition on BU device>	Displays the contents of the partition on the backup device. Requires the Crypto Officer PED key (BLACK).

Backup EPV
Initialize the second device, following the instructions above from Section 1, Step 3 – but there is no need to reset the timer if you do not want to. Using the keys we have already established, run through the PED device attached to the secondary HSM and when asked if you are using existing keys, **answer YES.**

***Follow the prompts on the PED carefully.**

Move the backup device to the secondary EPV and restore the partition/domain using the table below.

Partition Restore

Command	Explanation
If it is not already, Activate the slot that you will be restoring to. May require the PED and the Crypto Officer (BLACK) key and password	
Connect HSM BU device to your local PC via USB cable. Connect PED to HSM BU device.	
C:\Program Files\Safenet\LunaClient> lunacm lunacm:> slot list	List all available slots including the backup device
lunacm:> partition archive list -slot <slot# of Backup Device>	List the partitions on the backup Device
lunacm:> partition archive contents -slot <slot# of Backup Device> -partition <name of partition on BU device>	Displays the contents of the partition on the backup device. Requires the Crypto Officer PED key (BLACK).
lunacm:> partition archive restore -slot <slot# of Backup Device> -partition <name of partition on BU device> -password <crypto officer password>	Restores partition contents from the BU device to the Luna SA partition. Follow PED commands

Change Server Keys
Run ChangeServerKeys.exe

The program will prompt you for the directories of the old key's (from before you re-keyed the primary vault). Ensure you are providing the correct keys or else the program will error. If you are using the same Operator CD for this task, it will operate successfully.

Once this has run successfully, you can install PADR, start your backup server, and test replication.

Troubleshooting replication:
From Primary server, ensure to enable DR User and set password to Cyberark1 (same as when installed PADR Software.

From PADR or DR box: Turn off PA Server on DR box and attempt to turn on the PADR Service. Should start, if not…run createcredfile.exe user.cred and match password

Further Notes from proof of concept:

- We tested on the firmware that was shipped (6.2.1) which is FIPS 140-2 certified from 2013
- If we want to support the July 2015 firmware release (6.10.9) we would have to go through a lengthy process to upgrade This would be something the customer could be responsible to do.